

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL  
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication :

(à n'utiliser que pour les  
commandes de reproduction)

2 589 268

(21) N° d'enregistrement national :

86 14996

(51) Int Cl<sup>4</sup> : G 06 K 19/06 // G 07 F 7/10.

## DEMANDE DE BREVET D'INVENTION

A1

(12)

(22) Date de dépôt : 28 octobre 1986.

(30) Priorité : JP, 28 octobre 1985, n° 240 969/85 et 18 février 1986, n° 033 344/86.

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 18 du 30 avril 1987.

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : Société dite : KABUSHIKI KAISHA TOSHIBA. — JP.

(72) Inventeur(s) : Yasuo Iijima.

(73) Titulaire(s) :

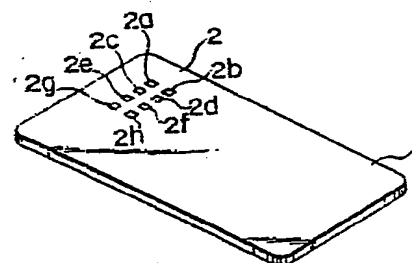
(74) Mandataire(s) : Cabinet Beau de Loménie.

(54) Dispositif électronique portatif sous forme d'une carte.

(57) L'invention concerne un dispositif électronique sous forme d'une carte électronique.

Elle se rapporte à une carte électronique 2 ayant des zones de contact 2a à 2h permettant la connexion à un système extérieur. Selon l'invention, la mémoire de la carte 2 contient plusieurs zones de données, contenant par exemple des numéros d'identification personnels, qui sont associés chacun à un nombre maximal de comparaisons pouvant donner un résultat négatif. Un numéro particulier d'identification est sélectionné, avec le nombre associé, lors de l'initialisation. De cette manière, deux mêmes cartes peuvent être utilisées pour des processus différents.

Application à la réalisation de cartes à mémoire pour transactions bancaires.



FR 2 589 268 - A1

La présente invention concerne un support portatif, par exemple une carte à circuit intégré comprenant des circuits paillettes tels qu'une unité centrale de traitement, une mémoire de données et analogues.

5 On a récemment mis au point une carte à circuit intégré qui est disponible dans le commerce sous forme d'une carte à mémoire destinée à conserver des données. Cette carte à circuit intégré comporte des circuits paillettes, par exemple une unité centrale de traitement, une mémoire  
10 de données qui constitue une mémoire passive programmable destinée à conserver un programme de commande et des données, et analogues. L'unité centrale est connectée à des bornes placées à la surface de la carte afin que la communication de données soit effectuée par l'inter-  
15 médiaire de ces bornes, et un accès de lecture-écriture de données à la mémoire est réalisé sous la commande de l'unité centrale.

Cependant, dans cette carte à circuit intégré, une limite de validité d'utilisation est fixée en fonction du  
20 domaine d'application ou du but recherché. La limite de validité d'utilisation comporte une date de validité, lorsque la carte est utilisée comme carte de crédit ou comme carte de passage, un montant limite lorsqu'elle est utilisée comme carte de distribution d'espèces, comme  
25 carte de crédit, comme carte téléphonique ou analogue, et la limite due à la capacité de la mémoire de la carte.

Les données mémorisées, par exemple des données de carte, une capacité actuelle de mémorisation ou une  
somme cumulée, doivent être lues par un dispositif extérieur  
30 destiné à juger de la limite de validité. Pour cette raison, diverses données conservées dans la carte à circuit intégré peuvent être atteintes depuis l'extérieur d'une manière facile, si bien que la sécurité est rendue plus difficile.

35 Un système bancaire mettant en oeuvre des cartes à circuit intégré comprenant des circuits paillettes a déjà été proposé. Les données utilisées pour la certifica-

tion de données d'identification personnelles lors d'une transaction sont enregistrées sur une bande magnétique placée à la surface d'une carte magnétique. Cette carte peut être facilement falsifiée ou des données peuvent être modifiées. Dans la carte à circuit intégré, les données de comparaison sont conservées dans la carte et ne peuvent pas être atteintes depuis l'extérieur. Les données d'identification personnelles introduites par un utilisateur sont certifiées par rapport à des données de comparaison mémorisées préalablement dans la carte et seul le résultat de la comparaison est transmis par la carte. Lorsqu'il existe un défaut de coïncidence, le nombre de défauts de coïncidence est compté. Lorsqu'il dépasse une valeur prédéterminée, la comparaison suivante est empêchée afin que la sécurité des données conservées dans la carte soit accrue.

Le nombre de défauts de coïncidence est comparé à une valeur prédéterminée à l'intérieur de la carte. Cependant, lorsque cette valeur prédéterminée est fixée par un programme de commande, une application dans laquelle la limite supérieure du nombre de défauts de coïncidence est obligatoirement différente n'est pas possible. En particulier, le programme de commande est conservé dans une mémoire passive cachée et ne peut pas être normalement lue depuis l'extérieur. Dans le cas précité, les cartes à circuit intégré qui conservent des programmes correspondant à des applications individuelles doivent être fabriquées séparément, si bien que la fabrication en grande série est difficile.

Lorsque la limite supérieure du nombre de défauts de coïncidence est fixée dans la mémoire de données de la carte à circuit intégré, lorsqu'elle peut être modifiée par l'utilisateur, la sécurité des données conservées dans la carte se trouve réduite.

La présente invention concerne un dispositif électronique portatif dans lequel des données mémorisées peuvent être facilement atteintes depuis l'extérieur.

Elle concerne aussi un dispositif électronique portatif qui peut déterminer de manière avantageuse le nombre de défauts de coïncidence correspondant à diverses applications lorsque le dispositif électronique est initialisé, si bien qu'un seul dispositif électronique portatif peut être utilisé pour diverses applications correspondant à des nombres différents de défauts de coïncidence, et, après initialisation du dispositif, le nombre de défauts de coïncidence ne peut pas être modifié et la sécurité peut être conservée.

Plus précisément, l'invention concerne un dispositif électronique portatif qui comprend une unité centrale de traitement et de commande, et une mémoire ayant une zone destinée à mémoriser des données de limite qui indiquent une limite de validité d'utilisation et une zone de mémorisation de données à traiter, l'unité centrale de traitement comparant les données de limite incorporées à des données de texte transmises par un système hôte connecté au dispositif électronique portatif, à des données de limite conservées dans la mémoire et déterminant si l'utilisation du dispositif électronique portatif est permis, et transmettant le résultat de son jugement.

D'autres caractéristiques et avantages de l'invention seront mieux compris à la lecture de la description qui va suivre d'exemples de réalisation, faite en référence aux dessins annexés sur lesquels :

la figure 1 est une perspective représentant l'aspect extérieur d'une carte à circuit intégré constituant un dispositif électronique portatif selon un mode de réalisation de l'invention ;

la figure 2 est un diagramme synoptique représentant un circuit électrique de la carte à circuit intégré de la figure 1 ;

la figure 3 représente l'organisation de la mémoire de données de la figure 2 ;

la figure 4 est une perspective indiquant l'aspect extérieur d'un appareil de manipulation de carte utilisé avec la carte de la figure 1 ;

la figure 5 est un diagramme synoptique du circuit de l'appareil de manipulation de carte de la figure 4 ;

la figure 6 est un format de texte échangé entre la carte et le manipulateur ;

5 la figure 7 est un format de bit de données de désignation de certification du type représenté sur la figure 6 ;

la figure 8 est une coupe d'un appareil de lecture-écriture de carte à circuit intégré ;

10 la figure 9 est un diagramme synoptique d'un circuit d'un appareil de lecture-écriture de carte à circuit intégré ;

les figures 10A à 10C son des ordinogrammes illustrant le fonctionnement d'un mode de réalisation de l'inven-  
15 tion ;

la figure 11 est un diagramme synoptique des blocs de fonction d'une carte à circuit intégré selon un autre mode de réalisation de l'invention ;

la figure 12 est un diagramme synoptique représentant l'arrangement de circuit paillette dans un autre mode de réalisation de l'invention ;

la figure 13 représente l'organisation de la mémoire de données du dispositif de la figure 12 ;

la figure 14 est un ordinogramme illustrant le fonctionnement d'un dispositif de surveillance ;

25 les figures 15A et 15B représentent des formats de données d'instruction ;

la figure 16 est un ordinogramme illustrant une opération de comparaison de numéro personnel d'identification ; et

30 la figure 17 représente le format de données d'instruction de comparaison de numéro personnel d'identification.

Sur la figure 1, la référence 1 désigne une carte à circuit intégré constituant un support portatif. Une section 2 formant connecteur est placée à la surface de la carte 1 et comporte plusieurs bornes 2a à 2h. La borne 2a

est utilisée comme borne d'alimentation (+ 5 V), la borne 2b comme borne de masse, la borne 2c comme borne de signaux d'horloge, la borne 2d comme borne de signaux de remise à zéro, les bornes 2e à 2g comme borne d'entrée-sortie de données, et la borne 2h comme borne d'alimentation d'écriture (+ 21 V).

La carte 1 à circuit intégré comporte une unité centrale de traitement 3, une mémoire de données 4 comprenant une mémoire passive programmable et effaçable électriquement EEPROM ou analogue, conservant un programme de commande et des données, un circuit 5 d'interface et une mémoire à accès direct 6 utilisé pour le traitement de données et conservant un texte transmis à un dispositif terminal (décrit dans la suite), comme représenté sur la figure 2. Les composants précités sont sous forme de circuits paillettes et sont disposés sur une même plaquette de circuit. Le circuit 5 d'interface est relié à la section 2 formant connecteur par un câblage.

La mémoire 4 de données comporte des zones 4a à 4f de mémorisation de données de limite dans lesquelles sont conservées diverses données de limite qui peuvent être utilisées comme limite de validité d'utilisation, introduites lors de la fabrication ou de la délivrance de la carte, et une zone 4g de conservation de données. Les zones 4a à 4f de mémorisation forment une zone 4a d'enregistrement destinée à conserver des données de temps, par exemple une date ou une heure, notamment une valeur d'expiration de données de temps, une zone 4b de conservation de données de temps, par exemple une date ou une heure, constituant une valeur d'avertissement d'expiration (ayant une valeur inférieure à la valeur d'expiration), une zone 4c de mémorisation d'une adresse finale, une zone 4d de mémorisation d'une adresse prédéterminée donnant une valeur d'avertissement de capacité de mémoire (ayant une valeur inférieure à celle de l'adresse finale), une zone 4e de conservation d'une valeur limite d'achat, et une zone 4f de conservation d'une valeur d'avertissement de limite d'achat (inférieure à la valeur limite d'achat).

Les figures 4 et 5 représentent un appareil 14 constituant un manipulateur de carte à circuit intégré formant un dispositif terminal selon la présente invention. Plus précisément, la référence 11 désigne une unité centrale de traitement destinée à commander l'ensemble de l'appareil, la référence 12 désigne un clavier destiné à l'introduction de données, la référence 13 une unité d'affichage à tube à rayons cathodiques, la référence 14 une mémoire passive conservant un programme de commande, la référence 15 une mémoire à accès direct destiné à conserver des données, la référence 16 une imprimante matricielle destinée à transmettre diverses données d'impression, la référence 17 une unité de disquette destinée à conserver et restituer des données sur une disquette 19 introduite par une ouverture 18 d'introduction de disquette, et la référence 20 une section de lecture-écriture de carte destinée à lire les données dans la zone 4g de mémorisation dans la mémoire 4 de la carte 1 introduite par l'ouverture 21 d'introduction de carte, et à écrire des données dans la zone 4g de la mémoire 4.

Un texte préparé dans l'unité centrale 11 et destiné à la carte 1 comporte un code de fonction des données de désignation de certification, des données de temps et des données de traitement comme l'indique la figure 6. Les données de désignation de certification sont formées de drapeaux destinés à indiquer si la certification est réalisée avec les données précitées de limite ou non. Par exemple, comme l'indique la figure 7, les données de désignation de certification ont une configuration à 8 bits. Lorsque le bit 0 (le plus significatif ou le moins significatif) est mis à un, cela indique la certification des données de temps (valeur d'expiration et valeur d'avertissement). Lorsque le bit 0 est mis à zéro, il indique que les données de temps ne doivent pas être certifiées. Lorsque le bit 1 est à un, il indique la certification d'une capacité de mémoire (valeur maximale et d'avertissement) et lorsque le bit 1 est à zéro, il indique

que la capacité de mémoire ne doit pas être certifiée. Lorsque le bit 2 est à un, il indique qu'une valeur limite d'achat doit être certifiée (valeur limite et valeur d'avertissement), et lorsqu'il est mis à zéro, il indique  
5 que la valeur ne doit pas être certifiée. Les données de désignation de certification sont préréglées pour chaque manipulateur 10 et sont conservées dans une mémoire interne (non représentée) de l'unité centrale 11.

La section 20 de lecture-écriture de carte à  
10 circuit intégré est connectée au manipulateur 10 par un câble 22. Plus précisément, comme l'indique la figure 8, la section 20 a un trajet 31 de transport de la carte 1 introduite par l'ouverture 21. Plusieurs paires de galets 32 de transport sont placées le long du trajet 31 afin  
15 que les galets soient disposés de part et d'autre de la carte 1 lorsqu'elle est transportée. Les paires de galets 32 sont placées à intervalles réguliers le long du trajet 31. La distance comprise entre le centre de chaque galet 32 de transport et le centre d'un galet adjacent 32  
20 correspond à la largeur de la carte 1 dans la direction de transport. En conséquence, le trajet 31 de la carte 1 est délimité par le guide 33 de transport.

Un dispositif de lecture-écriture 34 destiné à assurer la communication avec l'unité centrale 3 de la  
25 carte est placé au-dessus du guide 33. Ce dispositif 34 de lecture-écriture est relié électriquement à la section 2 formant connecteur.

Le circuit électrique de la section 20 de lecture-écriture de carte est placé comme représenté sur la figure  
30 9. Plus précisément, la section 20 comporte une unité centrale de traitement 51 destinée à commander l'ensemble de la section, une mémoire passive 52 qui conserve un programme de commande, une mémoire à accès direct 53 destinée à conserver des données, et le dispositif 34 de lecture-écriture.  
35

On décrit maintenant le fonctionnement de l'arrangement précité en référence aux figures 10A à 10C. On sup-

pose qu'un utilisateur introduit la carte 1 à circuit intégré dans l'ouverture 21. La carte 1 est reliée électriquement au dispositif 34 de lecture-écriture par la section 2 de connecteur. L'utilisateur introduit alors  
5 par exemple des données de transaction par l'intermédiaire du clavier 12. L'unité centrale 11 forme un texte constitué des données de temps lues dans une horloge interne (non représentée), d'un code de fonction correspondant aux données de désignation de certification et aux données  
10 de transaction, et des données de traitement, et les transmet à l'unité centrale 3 par l'intermédiaire du dispositif 34 de lecture-écriture de la section 20, de la section 2 de connecteur et du circuit 5 d'interface. L'unité centrale 3 reçoit le texte et le conserve dans  
15 la mémoire à accès direct 6. L'unité centrale 3 vérifie alors si le bit 0 des données de désignation de certification du texte est mis à 1 (pas 61 et 63). Lorsque la réponse du pas 63 est positive, l'unité centrale 3 détermine  
20 quelles données de temps (valeurs d'expiration et d'avertissement) doivent être certifiées. L'unité centrale 3 compare les données de date (données de temps) du texte conservé dans la mémoire 6 aux données de date (données de temps) conservées dans la zone 4a de mémoire parmi les zones  
25 de mémorisation de données de limite de la mémoire 4 (au pas 65). D'après le résultat de la comparaison, lorsque la date du texte a atteint la date de validité, l'unité centrale 3 détermine qu'une date de validité a expiré (pas 67) et transmet un texte qui l'indique à l'unité centrale  
30 de la date de validité de la carte introduite 1, affiche un message par l'intermédiaire de l'unité d'affichage 13 et retire alors la carte 1 ou la fait sortir par l'ouverture 21.

Cependant, lorsque l'unité centrale 3 détermine  
35 au pas 67 que la date du texte n'a pas atteint la date de validité, elle compare les données de date (données de temps) du texte conservé dans la mémoire 6 aux données de

date (données de temps) conservées dans la zone 4b parmi les zones de mémorisation de données de limite de la mémoire 4 (au pas 71). D'après le résultat de la comparaison, lorsque l'unité centrale 3 détermine au pas 73 que la date du texte a atteint une date ayant une valeur d'avertissement, elle transmet un texte indiquant ce phénomène à l'unité centrale 11 (pas 75), et le programme passe au pas 77. Ainsi, l'unité centrale 11 certifie que la valeur d'avertissement de la carte introduite 1 a été atteinte et affiche un message sur l'unité 13.

Cependant, lorsque l'unité centrale 3 détermine au pas 73 que la date du texte n'a pas atteint une date ayant une valeur d'avertissement, le programme passe au pas 77.

Lorsque l'unité centrale 3 détermine au pas 73 que la valeur d'avertissement n'est pas atteinte ou au pas 63 que les données de temps (valeurs d'expiration et d'avertissement) ne sont pas certifiées, l'unité centrale 3 vérifie si le bit 1 des données de désignation de certification du texte est à 1 (pas 77 et 79). Lorsque le pas 79 donne une réponse positive, l'unité centrale 3 détermine que la capacité de mémorisation (valeur maximale et d'avertissement) doit être vérifiée. L'unité centrale 3 compare les données de traitement du texte conservées dans la mémoire 6 à l'adresse finale (valeur maximale) conservée dans la zone 4c de mémorisation des zones de mémorisation de données de limite de la mémoire 4 (au pas 81). D'après cette comparaison, lorsque l'adresse finale est atteinte, l'unité centrale 3 détermine que la capacité de la mémoire 4 est complètement utilisée (pas 83) et transmet un texte indiquant ce phénomène à l'unité centrale 11 (pas 89). L'unité centrale 11 certifie ainsi que la capacité de mémorisation de la carte 1 est totalement occupée et l'indique sur l'unité 13. Simultanément, l'unité centrale 11 retire la carte 1 ou l'évacue par l'ouverture 21.

A la suite du résultat de la comparaison du pas 81, lorsque l'adresse finale n'est pas atteinte,

1 l'unité centrale 3 détermine que la capacité de la mémoire  
4 de données n'est pas totalement utilisée (pas 83) et  
compare les données de traitement du texte à une adresse  
prédéterminée (valeur d'avertissement) conservée dans la  
5 zone 4d des zones de mémorisation de données de limite  
de la mémoire 4 (au pas 85). Lorsque les données de trai-  
tement ont atteint l'adresse prédéterminée, l'unité centrale  
3 détermine que la capacité de la mémoire 4 a atteint  
la valeur d'avertissement (au pas 87), transmet un texte  
10 l'indiquant à l'unité centrale 11 (au pas 91) et le pro-  
gramme passe au pas 93. L'unité centrale 11 certifie  
alors que la capacité de mémorisation de la carte introduite  
1 a atteint la valeur d'avertissement et l'indique sur  
l'unité 13.

15 D'après le résultat de la comparaison du pas 85,  
lorsque l'adresse prédéterminée n'est pas atteinte, l'unité  
centrale 3 détermine que la capacité de la mémoire 4  
n'a pas atteint la valeur d'avertissement (au pas 87), et  
le programme passe au pas 93.

20 Lorsque l'unité centrale 3 détermine au pas  
87 que la capacité de la mémoire 4 n'a pas atteint la va-  
leur d'avertissement ou détermine au pas 79 que la capacité  
de mémorisation (valeurs maximale et d'avertissement)  
n'est pas certifiée, elle vérifie si le bit 2 des données  
25 de désignation de certification du texte conservé dans  
la mémoire 6 est au moins à 1 (au pas 93). Lorsque le  
bit 2 est à 1, l'unité centrale 3 détermine qu'une valeur  
limite d'achat (valeur limite et valeur d'avertissement)  
doit être certifiée (au pas 95). L'unité centrale 3 compare  
30 une valeur temporaire d'achat obtenue par addition des  
données de traitement du texte conservées dans la mémoire  
6 à une valeur d'achat conservée dans la zone 4g à une  
valeur d'achat (valeur limite) conservée dans la zone 4e (au  
pas 97). D'après le résultat de la comparaison, lorsque  
35 l'unité centrale 3 détermine au pas 99 que la valeur  
d'achat a atteint la valeur limite, elle transmet un texte  
l'indiquant à l'unité centrale 11 (au pas 107). L'unité

centrale 11 certifie alors que la valeur d'achat de la carte 1 a atteint la valeur limite, l'affiche sur l'unité 13, et retire la carte 1 ou l'évacue par l'ouverture 21.

5           Cependant, d'après le résultat de la comparaison du pas 97, lorsque l'unité centrale 3 détermine au pas 99 que la valeur temporaire d'achat n'atteint pas la valeur limite, elle conserve la valeur temporaire d'achat dans la zone 4g de mémorisation sous forme d'une nouvelle valeur d'achat (au pas 101). L'unité centrale 3 compare  
10   alors la nouvelle valeur d'achat à une valeur d'achat (valeur d'avertissement) conservée dans la zone 4f de mémorisation de valeur d'avertissement de limite d'achat 4f de la mémoire 4 (au pas 103). D'après le résultat de la comparaison du pas 103, lorsque l'unité centrale 3 détermine  
15   au pas 105 que la valeur d'achat a atteint la valeur d'avertissement, elle transmet un texte l'indiquant à l'unité centrale 11 (au pas 109). L'unité centrale 11 certifie que la valeur d'achat de la carte introduite 1 a atteint la valeur d'avertissement et l'affiche sur l'unité  
20   13.

          D'après le résultat de la comparaison du pas 103, lorsque l'unité centrale 3 détermine au pas 105 que la valeur d'achat n'a pas atteint la valeur d'avertissement, elle transmet un texte indiquant la fin du traitement à  
25   l'unité centrale 11 (au pas 111). L'unité centrale 11 certifie alors la fin du traitement de la carte 1 et évacue celle-ci par l'ouverture 21.

          Cependant, lorsque l'unité centrale 3 détermine au pas 95 que la valeur d'achat (valeur limite et valeur  
30   d'avertissement) n'est pas certifiée, elle effectue le traitement correspondant au texte mémorisé dans la mémoire 6, c'est-à-dire le traitement correspondant au code de fonction et aux données de traitement (au pas 113). Lorsque le traitement est terminé, l'unité centrale 3 transmet  
35   un texte indiquant la fin du traitement à l'unité centrale 11 (au pas 115). L'unité centrale 11 certifie alors la fin du traitement de la carte 1 et évacue celle-ci par l'ouverture 21.

Comme décrit précédemment, comme trois types d'opération de certification de limite sont réalisés de manière fiable et comme des données indiquant simplement la validité de la carte seulement sont transmises, les données détaillées conservées dans la carte peuvent être protégées par l'utilisateur ou le manipulateur et ne peuvent pas être connues par un tiers.

Un autre mode de réalisation de la présente invention est maintenant décrit en référence aux figures 11 à 16.

Une carte 1 à circuit intégré est possédée par un utilisateur et compare un numéro d'identification personnel connu uniquement de l'utilisateur ou accumule les données nécessaires, par exemple après l'achat d'un produit. Comme représenté par les blocs de fonction de la figure 11, la carte 1 comporte un bloc destiné à l'exécution de ces fonctions de base, par exemple une section 117 de lecture-écriture, une section 119 de détermination-comparaison de numéro personnel d'identification, une section 121 de chiffrement-déchiffrement et analogue, et un organe de surveillance 123 destiné à contrôler ces blocs de fonction fondamentaux. La section 117 de lecture-écriture est un bloc de fonction destiné à lire, écrire ou effacer des données, à l'aide de la section 20 de lecture-écriture de carte. La section 119 de détermination-comparaison de numéro personnel d'identification est un bloc de fonction destiné à conserver un numéro d'identification personnel déterminé par l'utilisateur et à empêcher l'accès à la lecture, et destiné à comparer le numéro d'identification personnel après sa détermination de manière que le traitement suivant soit possible. La section 121 de chiffrement-déchiffrement est un bloc de fonction destiné à chiffrer les données de communication lorsque des données sont transmises par l'unité centrale 11 à un autre dispositif terminal afin que les données soient protégées et ne puissent pas être connues ou modifiées par un tiers, la section assurant aussi le déchiffrement des données chiffrées. La section 121 exécute un traitement en fonction d'un algorithme de chiffrement ayant

une capacité suffisante de chiffage, par exemple suivant une norme de chiffage de données. L'organe 123 de surveillance est un bloc de fonction destiné à décoder un code de fonction avec ou sans entrée de données à partir de la  
5 section 20 de lecture-écriture, et il sélectionne la fonction nécessaire parmi les fonctions de base afin qu'elle soit remplie.

La carte 1 à circuit intégré de ce mode de réalisation, destinée à remplir ces fonctions, comporte une  
10 unité centale 125 de traitement, une mémoire permanente 127 qui permet l'effacement de son contenu, une mémoire 129 de programme, et un organe 131 de contact destiné à être en contact électrique avec la section 20 de lecture-écriture de carte, comme indiqué sur la figure 12. Parmi ces sec-  
15 tions, celles qui sont entourées par les traits interrompus (unité centrale 125, mémoire 127 de données et mémoire 129 de programme) sont constituées par des circuits paillettes. La mémoire 129 de programme est une mémoire passive cachée et conserve un programme de commande de l'unité centrale  
20 125, contenant des sous-programmes destinés à l'exécution des fonctions fondamentales. La mémoire 127 de données est utilisée pour la conservation des diverses données et est constituée par exemple d'une mémoire passive programmable et effaçable électriquement EEPROM. La mémoire  
25 127 de données est divisée en une zone 127<sub>1</sub> et une zone 127<sub>2</sub> de mémorisation de données spécifiées comme indiqué sur la figure 13. La zone 127<sub>1</sub> comprend une zone 127<sub>3</sub> destinée à conserver des numéros d'identifications personnels sous forme de plusieurs données de numéro d'identification  
30 personnel, les limites supérieures des nombres de défauts de coïncidence correspondant à ces numéros, et des données de zone, et une zone 127<sub>4</sub> de drapeau de fin d'initialisation. Les limites supérieures des nombres de défauts de coïncidence sont conservées lorsque la carte 1 est  
35 initialisée. L'unité centrale 125 détermine, d'après l'état du drapeau de fin d'initialisation, si l'initialisation de la carte 1 est terminée ou non.

Il faut noter que la figure 11 indique schématiquement les fonctions respectives de ce mode de réalisation de l'invention. L'organe 123 de surveillance de la figure 11 est réalisé par l'unité centrale 125 de la figure 12, et la section 117 de lecture-écriture, la section 119 de détermination-comparaison de numéro personnel d'identification et la section 121 de chiffrement-déchiffrement sont aussi réalisées par l'unité centrale 125 sous la commande d'un programme conservé dans la mémoire 129 de programme.

On considère maintenant le fonctionnement de l'unité centrale 125 en référence à l'ordinogramme de la figure 14, dans le cas de l'arrangement précédent. L'unité centrale 125 reçoit des données d'instruction représentées sur la figure 15A ou 15B, au pas 133, les déchiffre et les exécute. Les données d'instruction ne comportent qu'un code de fonction comme indiqué sur la figure 15A ou comporte un code de fonction et des données ajoutées comme indiqué sur la figure 15B. Le code de fonction peut être considéré comme un code exécuté lors de l'initialisation ou comme un code exécuté après la fin de l'initialisation. Lorsque les données d'instruction sont transmises à la carte 1, l'unité centrale 125 détermine, d'après le code de fonction qui y est compris, si les données d'instruction sont destinées à l'initialisation. Lorsque la réponse au pas 135 est positive, l'unité centrale 125 se réfère à la zone 127<sub>4</sub> de drapeau de fin d'initialisation au pas 137 et vérifie si l'initialisation est terminée. Lorsque la réponse du pas 137 est positive, l'unité centrale 125 transmet des données de réponse indiquant une erreur d'instruction au pas 139, et le programme revient alors au pas 133. Lorsque la réponse au pas 137 est négative, l'unité centrale 125 exécute les données d'instruction et transmet des données de réponse indiquant la fin de l'exécution au pas 141, et le programme revient au pas 133. Cependant, lorsque la réponse au pas 135 est négative, l'unité centrale 125 se réfère à la zone 127<sub>1</sub> de drapeau de fin d'initialisation au pas 143. Lorsque la réponse du pas 143 est négative, l'unité centrale 125 crée des données en réponse indiquant

une erreur d'instruction au pas 139. Cependant, lorsque la réponse est positive au pas 143, l'unité centrale 125 exécute ces données d'instruction, transmet des données de réponse indiquant que l'instruction a été exécutée, et le programme revient alors au pas 133. Lorsque les données d'instruction destinées à déterminer la limite supérieure du nombre de défauts de coïncidence sont considérées comme des données d'initialisation, la limite supérieure peut être avantageusement fixée pendant l'initialisation. Lorsque l'initialisation est terminée, la limite supérieure ne peut plus être remise à jour. En conséquence, la limite supérieure du nombre de défauts de coïncidence ne peut pas être modifiée depuis l'extérieur.

On décrit maintenant l'opération de comparaison de numéro d'identification personnel en référence à l'ordinogramme de la figure 16. Les données d'instruction de comparaison de numéro personnel d'identification comprennent le code 145 de fonction de comparaison, des données 147 de zone et des données 149 de comparaison comme l'indique la figure 17. Lorsque l'unité centrale 125 reçoit ces données d'instruction au pas 151 elle recherche le même index que celui qui est compris dans les données d'instruction provenant de la zone 127<sub>3</sub> de numéro personnel d'identification, au pas 153. Lorsque de telles données ne sont pas trouvées au pas 155, l'unité centrale 125 transmet des données de réponse indiquant l'impossibilité de l'exécution au pas 157 et le programme revient au pas 151. Lorsque des données sont trouvées au pas 155, des données de numéro d'identification personnel de la zone 127<sub>3</sub> correspondant à l'index sont comparées aux données de comparaison introduites, au pas 159. Lorsqu'une coïncidence est déterminée au pas 161, l'unité centrale 125 transmet des données de réponse indiquant que l'utilisation de la carte est permise au pas 163. Cependant, lorsqu'une coïncidence n'est pas déterminée au pas 161, l'unité centrale 125 détermine le nombre de défauts de coïncidence au pas 165. Lorsque le nombre actuel de défauts de coïncidence n'a pas atteint la

limite supérieure indiquée dans la zone 127<sub>3</sub>, comme déterminé au pas 165, l'unité centrale 125 crée des données de réponse indiquant le défaut de coïncidence, au pas 167, et le programme revient au pas 151. Lorsque le pas 165 détecte  
5 que le nombre de défauts de coïncidence a atteint la limite supérieure, l'unité centrale 125 crée des données de réponse indiquant que l'utilisation de la carte est empêchée au pas 169 si bien que l'acceptation de données suivantes d'instruction est empêchée.

10 De cette manière, comme la limite supérieure du nombre de défauts de coïncidence du nombre d'identification personnel de la carte à circuit intégré peut être déterminée avantageusement lors de l'initialisation, une même carte à circuit intégré peut être utilisée dans diverses applica-  
15 tions nécessitant des limites supérieures différentes. En outre, comme la limite supérieure ne peut pas être modifiée lorsque la carte a été initialisée, la sécurité du système de gestion par carte à circuit intégré peut être garantie.

Dans le mode de réalisation qui précède, la  
20 mémoire de données est une mémoire passive programmable et effaçable électriquement, mais il peut aussi s'agir d'une mémoire à accès direct ou d'une mémoire passive programmable électriquement.

Dans le mode de réalisation qui précède, la carte  
25 à circuit intégré a été considérée comme constituant un dispositif électronique portatif. Cependant, la configuration du dispositif électronique portatif n'est pas limitée à celle d'une carte, mais il peut s'agir d'une configuration analogue à un bloc ou un crayon. Les circuits du dispositif  
30 électronique portatif peuvent être modifiés dans le cadre de l'invention.

Bien entendu, diverses modifications peuvent être apportées par l'homme de l'art aux dispositifs qui viennent d'être décrits uniquement à titre d'exemples  
35 non limitatif sans sortir du cadre de l'invention.

REVENDECATIONS

1. Dispositif électronique portatif, caractérisé en ce qu'il comprend :
- 5           une unité centrale de traitement (3), et  
          une mémoire (4) ayant une zone (4a à 4f) de mémorisation de données de limite indiquant une limite de validité d'utilisation, et une zone (4g) de mémorisation de données à traiter, l'unité centrale de traitement comparant des données de limite comprises dans des données de texte transmises par un système hôte connecté au dispositif électronique portatif à des données de limite conservées dans la mémoire, déterminant si l'utilisation du dispositif électronique portatif est permis, et transmettant le résultat de sa détermination.
- 10           2. Dispositif selon la revendication 1, caractérisé en ce que la mémoire est une mémoire passive programmable.
- 15           3. Dispositif selon la revendication 1, caractérisé en ce que la mémoire est une mémoire passive électriquement effaçable.
- 20           4. Dispositif selon la revendication 1, caractérisé en ce que la zone de mémorisation des données de limite comporte une zone (4a) de mémorisation d'une valeur d'expiration de données de temps, et une zone (4b) de mémorisation d'une valeur d'expiration avancée de données de temps indiquant une valeur d'avertissement de limite.
- 25           5. Dispositif selon la revendication 1, caractérisé en ce que la zone de mémorisation des données de limite comporte une zone (4e) de mémorisation d'une valeur limite de possibilité d'achat, et une zone (4f) de mémorisation d'une valeur d'avertissement de limite de possibilité d'achat, inférieure à la valeur limite de possibilité d'achat.
- 30           6. Dispositif selon la revendication 1, caractérisé en ce que la zone de mémorisation de données de limite comporte une zone de mémorisation d'une valeur d'expiration de données de temps, une zone de mémorisation d'une valeur d'expiration avancée de données de temps indiquant une
- 35

valeur d'avertissement de limite, une zone de mémorisation d'une valeur limite de capacité d'achat, et une zone de mémorisation d'une valeur d'avertissement de limite de capacité d'achat inférieure à la valeur limite de capacité d'achat.

7. Dispositif selon l'une quelconque des revendications 4 à 6, caractérisé en ce que la zone de mémorisation de données de limite comporte en outre une zone (4c) de mémorisation d'une valeur de limite de capacité de mémoire, et une zone (4d) de mémorisation d'une valeur d'avertissement de limite de capacité de mémoire inférieure à la valeur limite de capacité de mémoire.

8. Dispositif selon la revendication 7, caractérisé en ce que les données de texte échangées entre le dispositif électronique portatif et le système hôte qui lui est connecté sont constituées d'un code de fonction destiné à indiquer une fonction à exécuter par le dispositif électronique portatif, les données de désignation de certification, des données de temps, et des données de traitement, et les données de désignation de certification ont des données de drapeau de certification de données de temps indiquant si les données de temps doivent être certifiées, un drapeau de certification de capacité d'achat indiquant si la capacité d'achat doit être certifiée, et un drapeau de certification de capacité de mémoire indiquant si la capacité de la mémoire doit être certifiée.

9. Dispositif électronique portatif selon la revendication 1, caractérisé en ce que la mémoire conserve des données de nombre prédéterminé destinées à une comparaison, l'unité centrale de traitement compare les données d'identification personnelles transmises par le système hôte connecté au dispositif électronique portatif à des données d'identification personnelles conservées dans la mémoire, et, lorsque le nombre de défauts de coïncidence détecté par l'unité centrale de traitement dépasse les données de nombre prédéterminé conservées dans la mémoire, l'unité centrale de traitement empêche le traitement suivant de comparaison.

10. Dispositif selon la revendication 9, caractérisé en ce que les données de nombre prédéterminé peuvent être conservées dans la mémoire uniquement lors de l'initialisation du dispositif électronique portatif, et ne peuvent pas être modifiées après la fin de l'initialisation.

11. Dispositif selon la revendication 10, caractérisé en ce que la mémoire est divisée en une zone de mémorisation de données spécifiées et une zone de mémorisation de données, et la zone de mémorisation de données spécifiées contient une zone destinée à mémoriser des numéros d'identification personnels sous forme de plusieurs données d'identification personnelles, des limites supérieures de nombre de défauts de coïncidence correspondant aux numéros respectifs d'identification personnels, et des données de zone, ainsi qu'un drapeau de fin d'initialisation.

12. Dispositif selon la revendication 11, caractérisé en ce que l'unité centrale de traitement détermine si l'initialisation du dispositif électronique portatif a été terminée ou non en se référant au drapeau de fin d'initialisation, et, lorsque l'initialisation n'est pas terminée, l'unité centrale de traitement détermine la limite supérieure du nombre de défauts de coïncidence alors que, lorsque l'initialisation a été déterminée, l'unité centrale de traitement empêche la modification de la limite supérieure du nombre de défauts de coïncidence.

1/12

FIG. 1

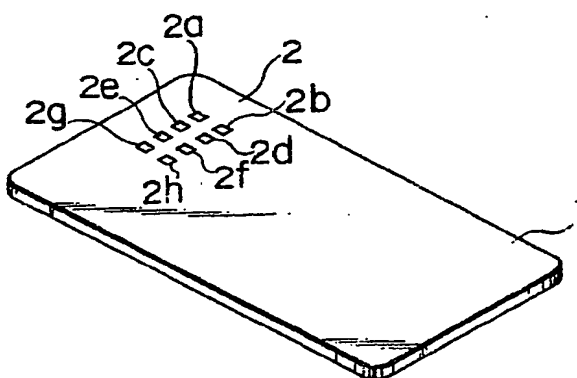
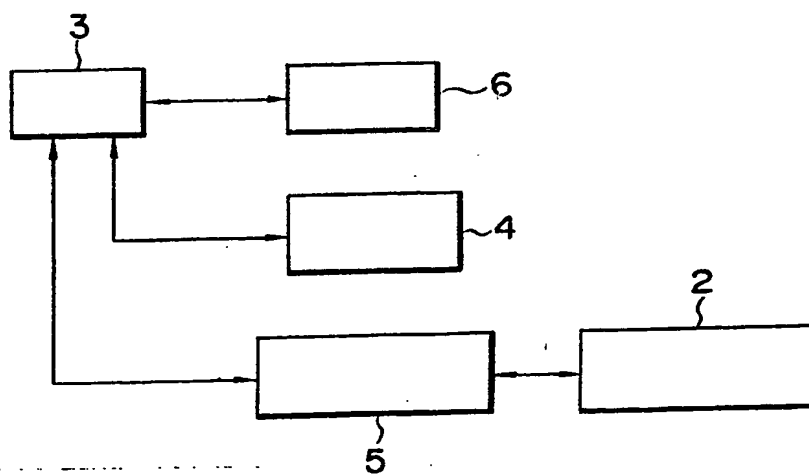


FIG. 2



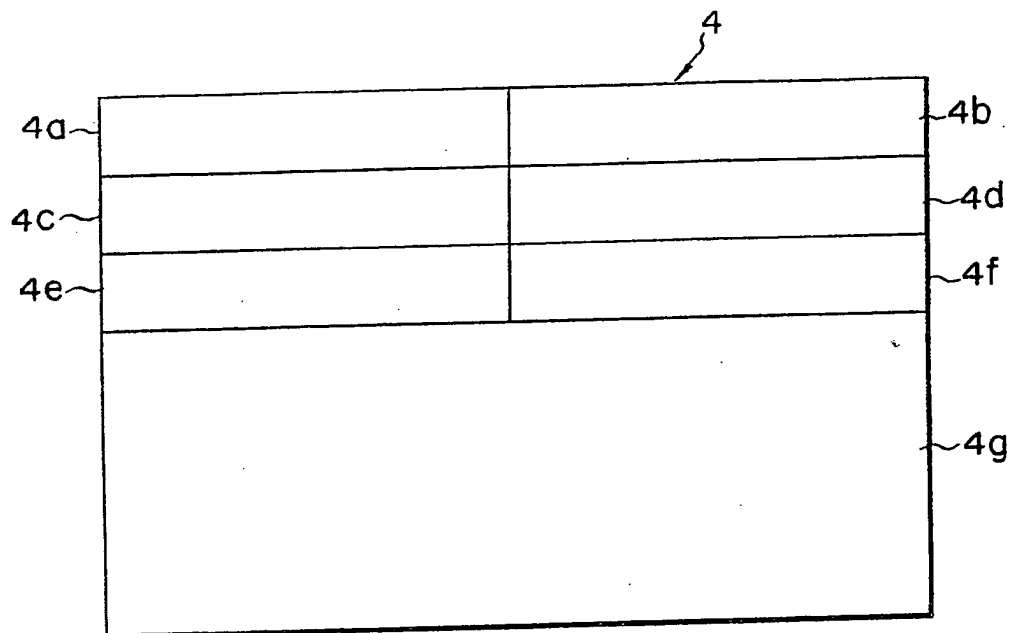
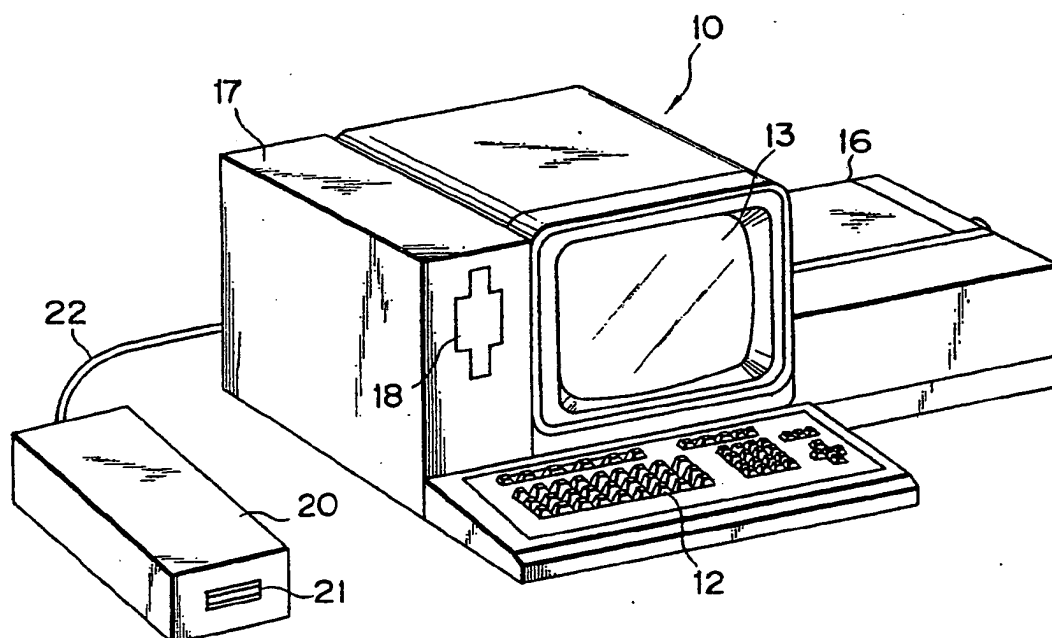
2/12  
FIG. 3

FIG. 4



3/12  
FIG. 5

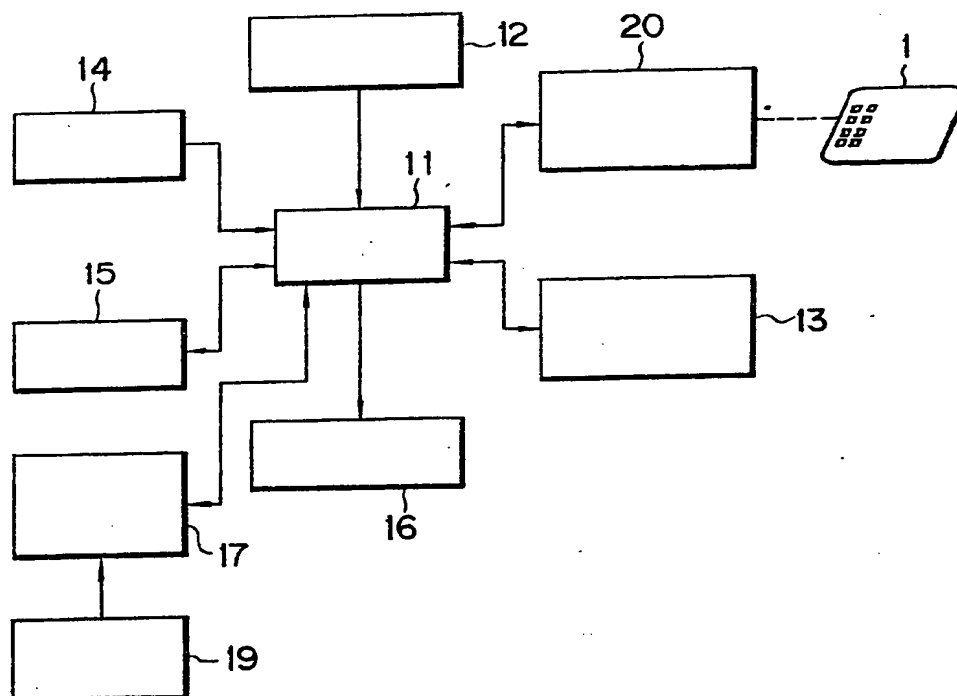


FIG. 6

Code Fonction	Données dési- gnation Certification	Données de temps	Données de traitement
------------------	---	---------------------	-----------------------------

FIG. 7

7	6	5	4	3	2	1	0
X	X	X	X	X	0	1	1

4/12

FIG. 8

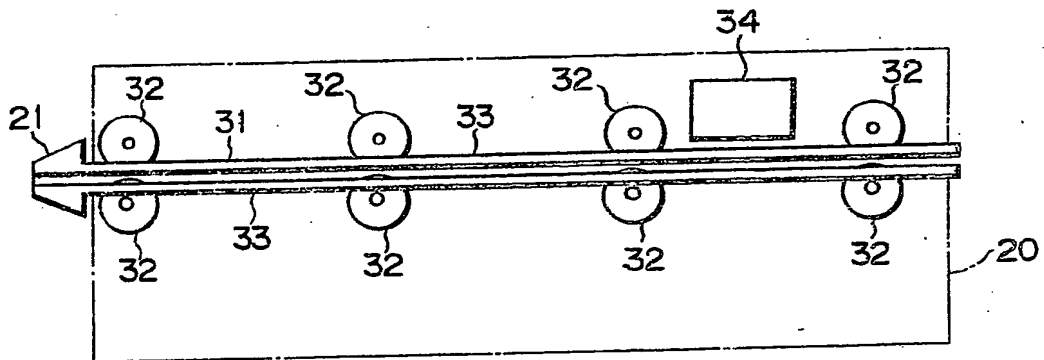
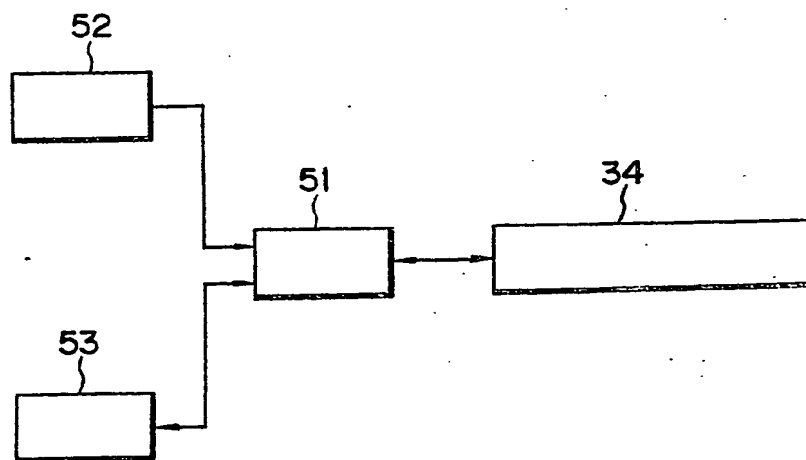
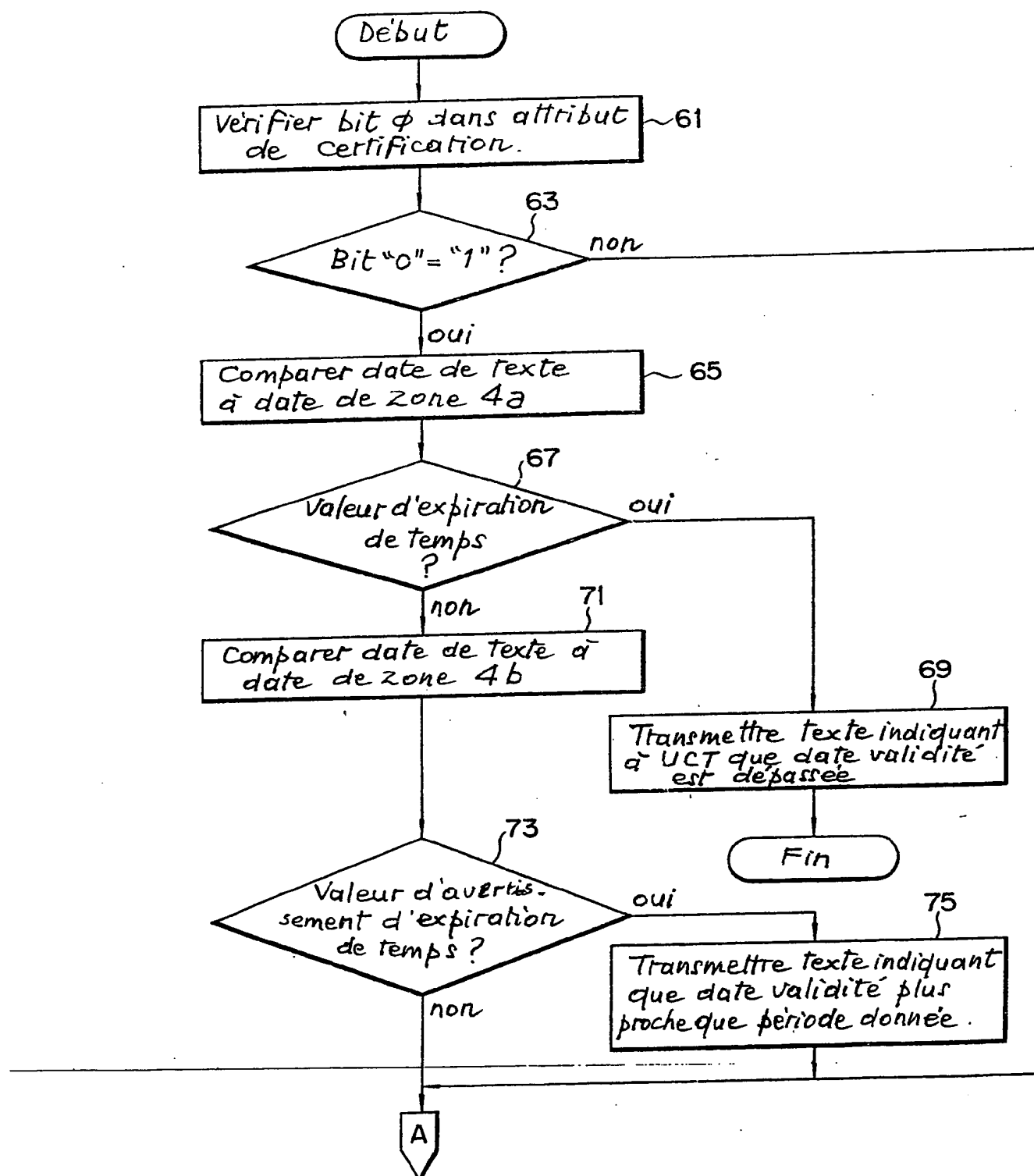


FIG. 9



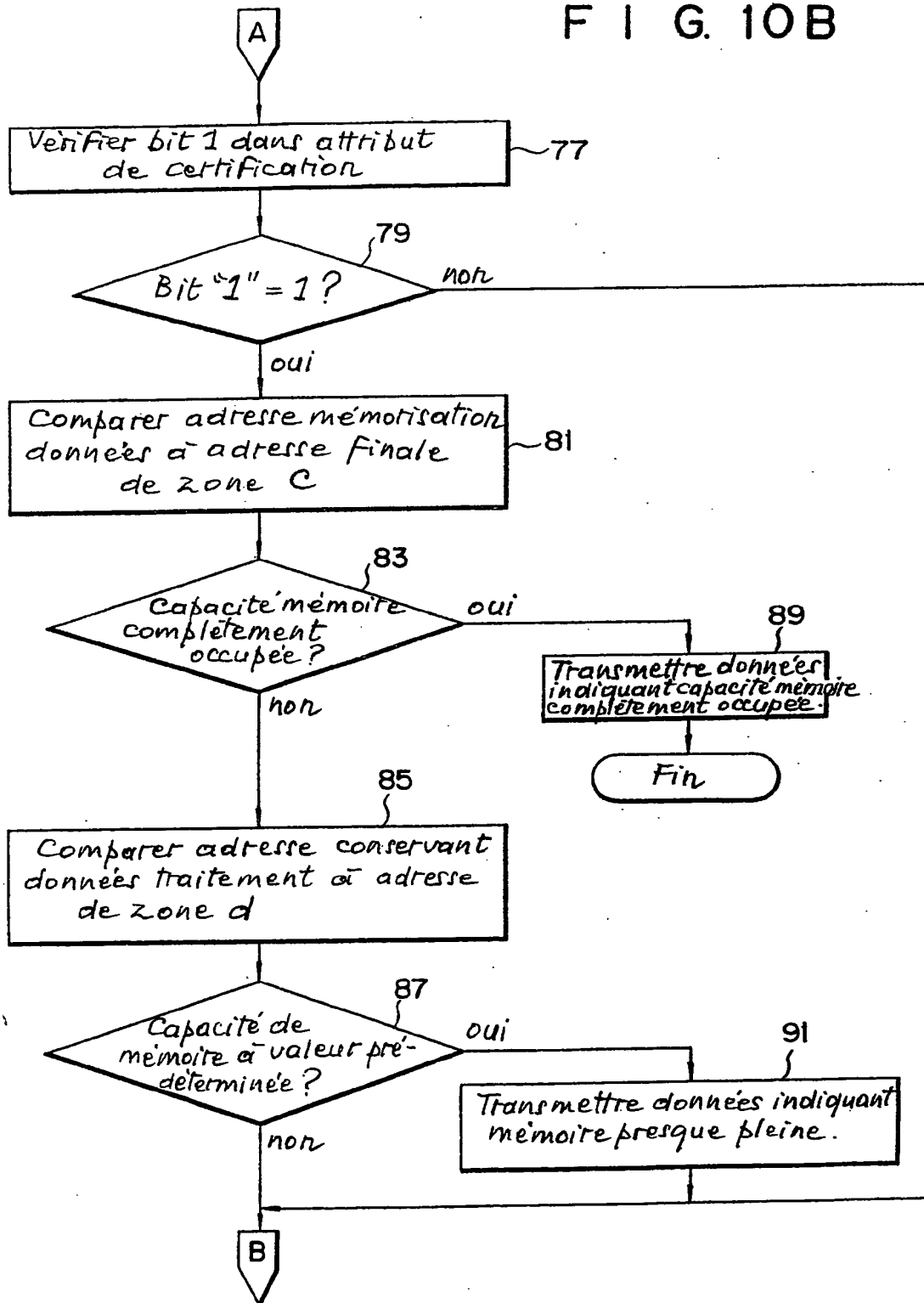
5/12

F I G. 10A



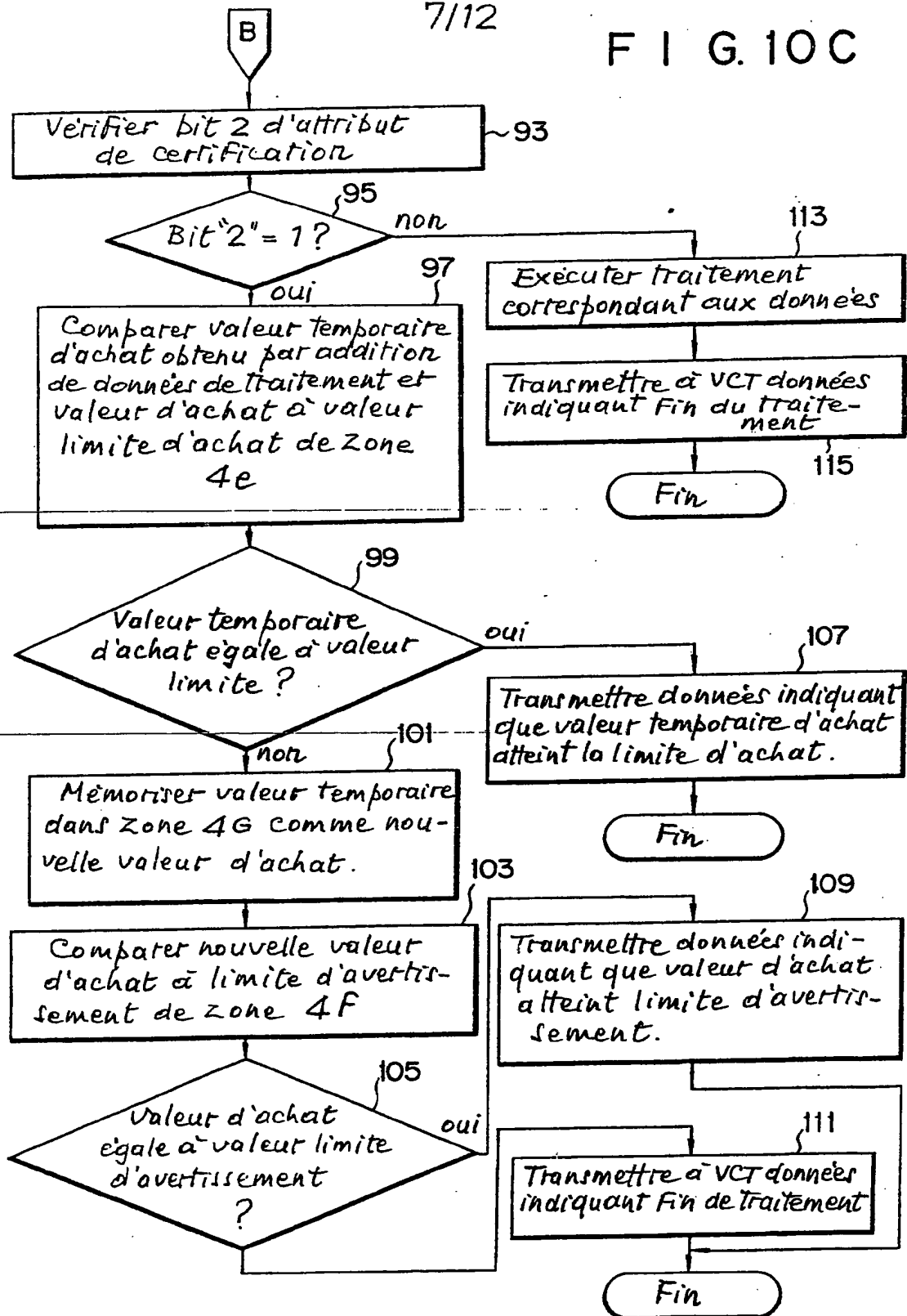
6/12

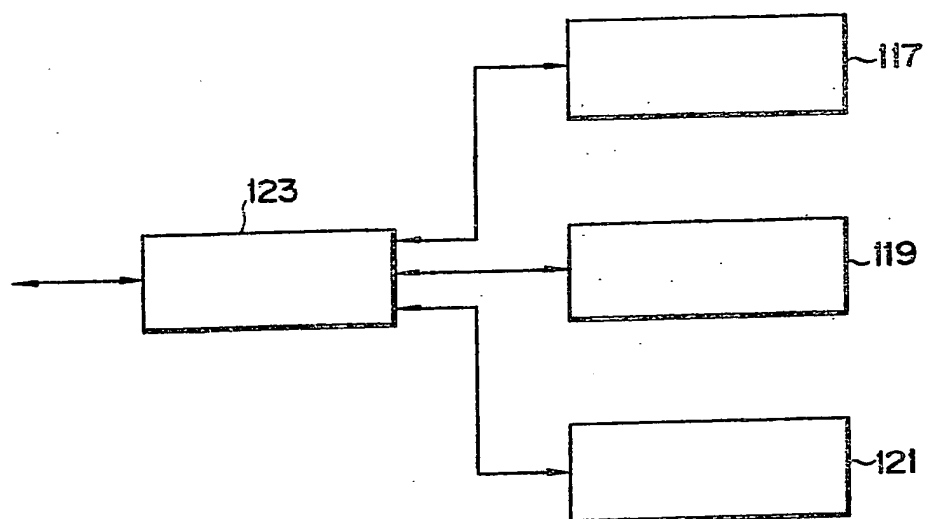
F I G. 10B



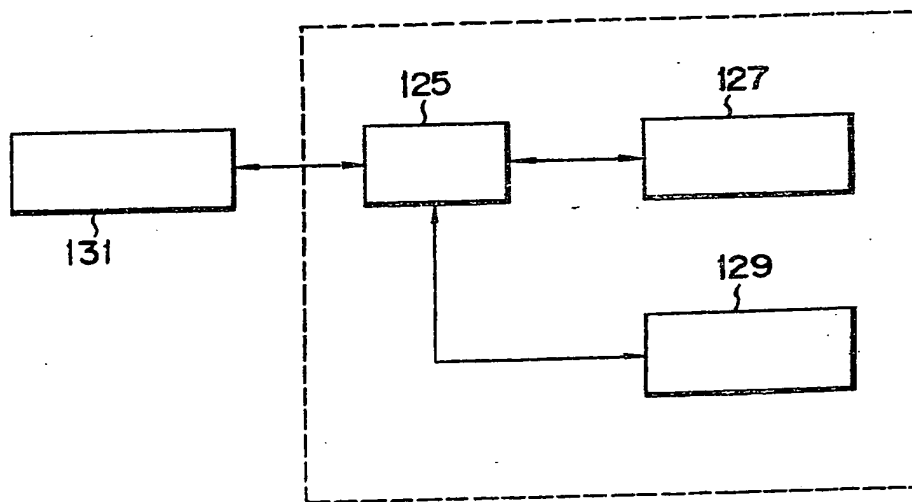
7/12

F I G. 10C



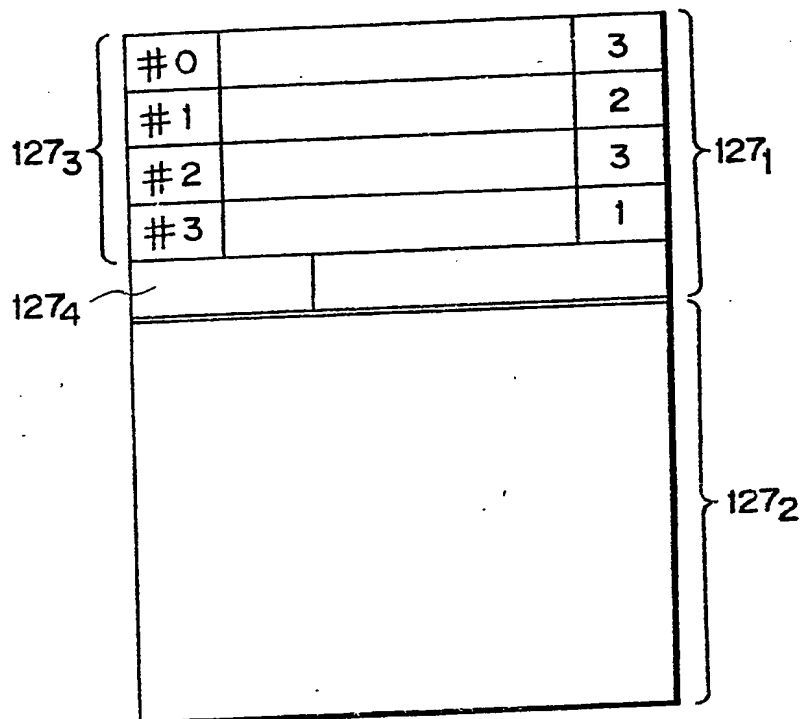
8/12  
F I G. 11

F I G. 12



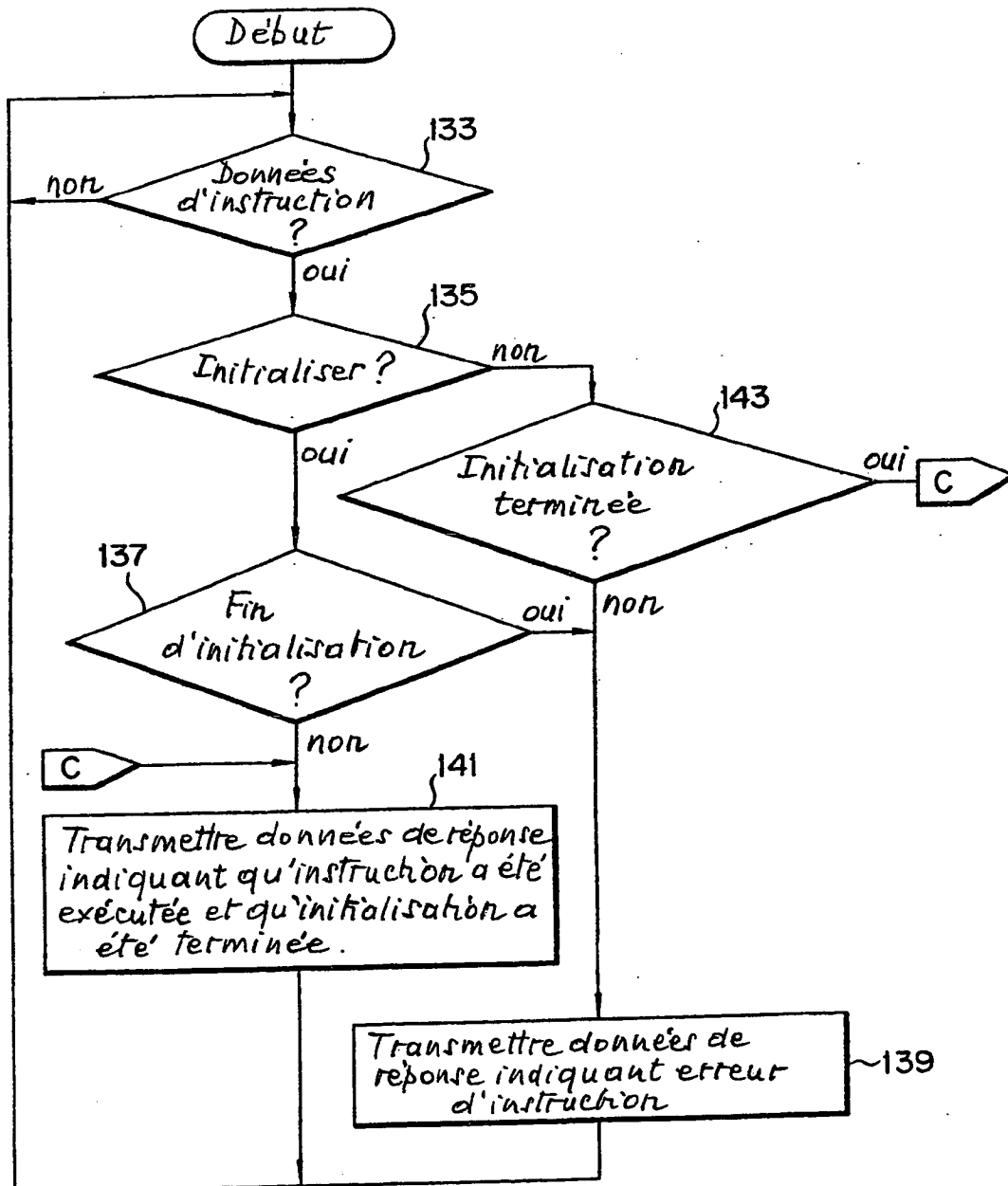
9/12

FIG. 13



10/12

## FIG. 14



11/12

F I G. 15A

Code de fonction
---------------------

F I G. 15B

Code de Fonction	Données
---------------------	---------

F I G. 17

145 }	147 }	149 }

12/12  
FIG. 16